
FORTINET
High Performance Network Security
FortiWLC
Release 8.4.0
SSL
IPsec

With this release of FortiWLC-SD, the FAP-U221EV, FAP-U223EV, FAP-U24JEV, and FAP-U422EV access points are introduced.
For more information on setting up the FAPs, see the related *Quick Start Guides*.
This release also provides some enhancements on the existing FortiWLC functionalities (New Features and Enhancements).

Getting Started with Upgrade

The following table describes the approved upgrade path applicable for all controllers except the new virtual controllers.

NOTE:
FortiWLC-1000D and FortiWLC-3000D controllers can be upgraded only from 8.3 releases.

Supported Upgrade Releases

From FortiWLC release…	To FortiWLC Release…
7.0	7.0-10-0
8.0	8.0-5-0, 8.0-6-0
8.1	8.1-3-2
8.2	8.2.4
8.2.4/8.3	8.3.1
7.0.11, 8.2.7, 8.3.0, 8.3.1, and 8.3.2	8.3.3
7.0-11, 8.2.7, 8.3.0, 8.3.1, 8.3.2, 8.3.3	8.4.0

NOTE:

- Fortinet recommends that while upgrading 32-bit controllers to version 8.4.0, use the **upgrade controller** command instead of the **upgrade system** command.
- Controller upgrade performed via CLI interface will require a serial or SSH2 connection to connect to the controller and use its CLI. FortiWLC-1000D and FortiWLC-3000D controller upgrades can be performed via GUI as well.

Check Available Free Space

Total free space required is the size of the image + 50MB (approximately 230 MB). You can use the **show file systems** command to verify the current disk usage.

```
controller# show file systems
Filesystem     1K-blocks   Used        Available   Use%   Mounted on
/dev/hdc2      428972      227844    178242      57%      /
none               4880           56            4824           2%       /dev/shm
```

The first partition in the above example, /hdc2, although the actual name will vary depending on the version of FortiWLC-SD installed on the controller is the one that must have ample free space.

In the example above, the partition shows 178242KB of free space (shown bolded above), which translates to approximately 178MB. If your system does not have at least 230MB (230000KB) free, use the **delete flash:<flash>** command to free up space by deleting older flash files until there is enough space to perform the upgrade (on some controllers, this may require deleting the flash file for the current running version).

Set up Serial Connection

Set the serial connection for the following options:

NOTE:
Only one terminal session is supported at a time. Making multiple serial connections causes signalling conflicts, resulting in damage or loss of data.

- Baud--115200
- Data--8 bits
- Parity--None
- Stop Bit—1
- Flow Control—None

Supported Hardware and Software

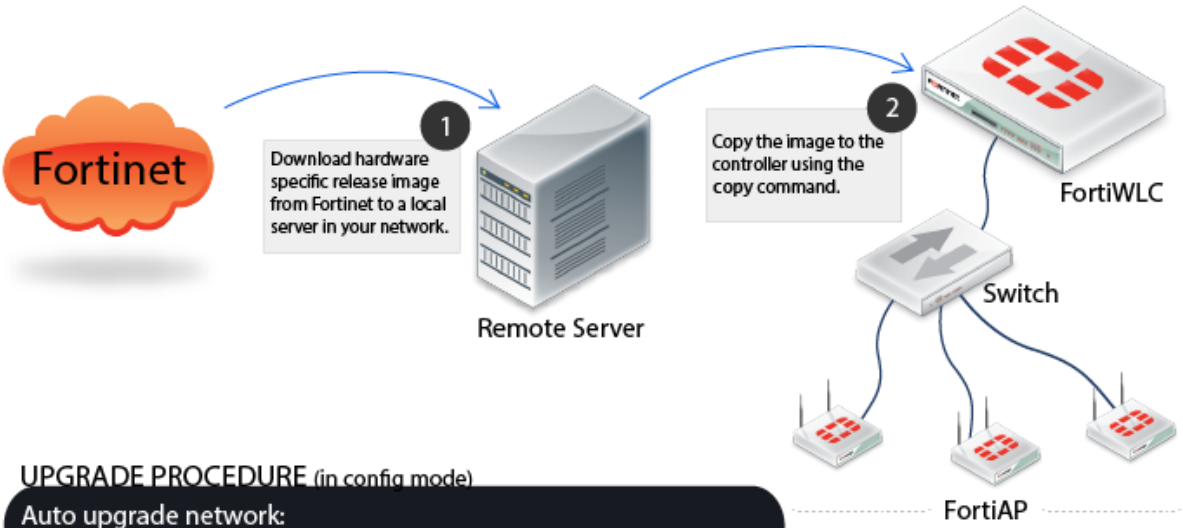
This table lists the supported hardware and software versions in this release of FortiWLC.

Hardware and Software	Supported		Unsupported
Access Points	AP122 AP822e, AP822i (v1 & v2) AP832e, AP832i, OAP832e AP332e* AP332i* AP433e* AP433i* OAP433e* FAP-U421EV FAP-U423EV FAP-U321EV FAP-U323EV FAP-U422EV	FAP U221EV FAP U223EV FAP U24JEV AP1010e* AP1010i* AP1020e* AP1020i* AP1014i* AP110*	AP201 AP208 AP150 AP300, AP301, AP302, AP302i, AP301i AP310, AP311, AP320, AP310i, AP320i OAP180 OAP380
*Cannot be configured as a relay AP			
Controllers	FortiWLC-50D FortiWLC -200D FortiWLC -500D FortiWLC- 1000D# FortiWLC -3000D# FWC- VM-50# FWC –VM-200# FWC –VM-500# FWC –VM-1000# FWC-VM-3000#	MC3200, MC3200-VE MC1550, MC1550-VE MC6000 MC4200 (with or without 10G Module) MC4200-VE	MC 5000 MC 4100 MC 1500 MC 1500-VE
#Spectrum Manager NOT supported in these controller models.			
FortiWLM	8.3.3/8.4		
FortiConnect	16.8.2		
Browsers			
FortiWLC (SD) WebUI	Internet Explorer 9,10 Mozilla Firefox 25+ Google Chrome 31+		
NOTE: A limitation of Firefox 3.0 and 3.5+ prevents the display of the X-axis legend of dashboard graphs.			

Captive Portal	Internet Explorer 6, 7, 8, 9, 10, IE11 and Edge. Apple Safari Google Chrome Mozilla Firefox 4.x and earlier Mobile devices (such as Apple iPhone and BlackBerry)	

Installing and Upgrading

Follow this procedure to upgrade FortiWLC-50D, FortiWLC-200D, FortiWLC-500D, MC1550, MC1550-VE, MC3200, MC3200-VE, MC4200, MC4200-VE and MC6000 controllers. See section Upgrading FortiWLC-1000D and FortiWLC-3000D to upgrade FortiWLC-1000D and FortiWLC-3000D. See Upgrading Virtual Controllers to upgrade virtual controllers.



UPGRADE PROCEDURE (in config mode)

Auto upgrade network:
To upgrade controllers and APs

```
#upgrade system <target-version>
```

Phase upgrade:
To upgrade controllers first and then all APs

```
#auto-ap-upgrade disable
#upgrade controller <target-version>
#upgrade ap same all OR upgrade ap same <ap-ID>
```

Step upgrade:
To upgrade controllers and then auto upgrade all APs

```
#auto-ap-upgrade enable
#upgrade controller <target-version>
```

Patch upgrade:
To upgrade controllers to a patch release

```
#patch install <target-patch/version>
```

1. Download image files from the remote server to the controller using one of the following commands:

   ```
   # copy ftp://ftpuser:<password@ext-ip-addr>/<image-name-rpm.tar><space>.
   ```

   [OR]

   ```
   # copy tftp://<ext-ip-addr>/<image-name-rpm.tar><space>.
   ```

   Where

   - *image-name* for legacy controllers: meru-{release-version}-{hardware-model}-rpm.tar. Eg, meru-8.3-3-MC4200-rpm.tar

- *image-name* for FortiWLC: forti-{release-version}-{hardware-model}-rpm.tar. Eg, forti-8.3-3-FWC2HD-rpm.tar

2. Disable AP auto upgrade and then upgrade the controller (in config mode)

```
# auto-ap-upgrade disable

# copy running-config startup-config

# upgrade controller <target version> (Example, upgrade controller 8.3)
```

   The *show flash* command displays the version details.

3. Upgrade the APs

```
# upgrade ap same all
```

After the APs are up, use the *show controller* and *show ap* command to ensure that the controller and APs are upgraded to the latest (upgraded) version. Ensure that the system configuration is available in the controller using the *show running-config* command (if not, recover from the remote location). See the Backup Running Configuration step.

Upgrading FortiWLC-1000D and FortiWLC-3000D

To upgrade to FortiWLC-1000D and FortiWLC-3000D, use the following instructions.

In version 8.4.0, the image naming systems have been changed for 64 bit controller models from Primary/Secondary to image0/image1. This change applies to the upgrade procedure in the related FortiWLC GUI screens and CLI commands.

Upgrading via CLI

1. Use the **show images**command to view the available images in the controller. By default, a new controller will boot from the primary partition which contains the running image.

```
default(15)# show images
Running image: Primary   <---- Denotes Primary Partition
--------------------------------------------------------------------------------
Running image details.
         System version: 0.3.2
         System hash: 11af7a3f3a700d3c8335dc254165282a91bd021b
         System branch: master
         System built: 20170323191620
         System memory: 721M/1006M
         Apps version: 8.3-1build-15
         Apps size: 1204M/1822M
--------------------------------------------------------------------------------
Other image details.
         System version: 0.3.3
         System hash: 4699cb9f517c4a2abbbce458f689bf3558b5d65e
         System branch: master
         System built: 20170511180827
         System memory: 729M/1015M
         Apps version: 8.3-1build-21
```

```
Apps size: 1119M/1821M
```

2. To install the latest release, download the release image using the *upgrade-image* command:

```
upgrade-image scp://<username>@<remote-server-ip>:<path-to-image>/<image-name>-rpm.tar both

reboot
```

The above command will upgrade the secondary partition and the controller will reboot to secondary partition.

NOTE:

After an upgrade the current partition will shift to the second partition. For example, if you started upgrade in primary partition, post upgrade the default partition becomes secondary partition and vice- versa.

```
default(15)# show images
    Running image: Secondary  <--- Current partition after upgrade
    ------------------------------------------------------------------------
    ---------
    Running image details.
             System version: 0.3.2
             System hash: 11af7a3f3a700d3c8335dc254165282a91bd021b
             System branch: master
             System built: 20170323191620
             System memory: 729M/1015M
             Apps version: 8.3-1build-20
             Apps size: 1116M/1821M
    ------------------------------------------------------------------------
    ---------
    Other image details.
             System version: 0.3.2
             System hash: 11af7a3f3a700d3c8335dc254165282a91bd021b
             System branch: master
             System built: 20170323191620
       System memory: 721M/1006M
       Apps version: 8.3-1build-15

        Apps size: 1204M/1822M
```

Upgrading via GUI

This section describes the upgrade procedure through the FortiWLC GUI.

NOTE:

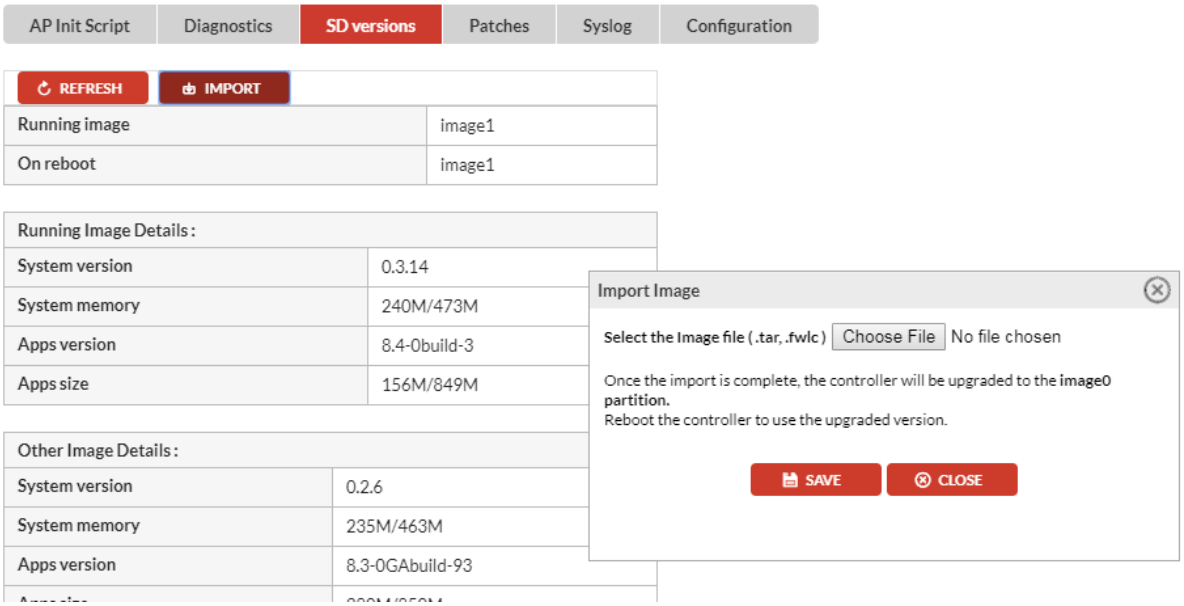
- Standalone controllers running pre-8.3.3 FortiWLC (except version **7.0-12**) are **required** to upgrade to 8.3.3 GA and then to the current 8.4.0 version.
  Fortinet recommends upgrading via CLI to avoid this issue which occurs due to file size limitation.
- This issue does not exist on controllers with manufacturing build as 8.3.3 GA.

1. To upgrade controllers using GUI, navigate to *Maintenance > File Management > SD Version*.
2. Click *Import* button to choose the image file.

NOTE:

FortiWLC release 8.4.0 introduces software upgrades using the *.fwlc* format. This format will be supported in the forthcoming releases.

Direct upgrade from a pre-8.4.0 to 8.4.0 release using the *.fwlc* format is not supported.



3. After the import is complete, a success message is displayed.

Switching Partitions

To switch partitions in FortiWLC-1000D, FortiWLC-3000D and the new virtual controllers, select the partition during the bootup process.

Upgrading 32-bit 8.3.3 Controllers (MC models, FortiWLC-50D/200D/500D) with AP832/822 (without KRACK patch)

Upgrading from FortiWLC 8.3.3 to 8.4.0 results in *runtime1* image corruption in AP832 and AP822v1. This is due to a resource leak in the 8.3.3 version which is fixed in later releases.

Follow these steps to upgrade from 8.3.3 to 8.4.0.

1. Reboot the APs before upgrade.
2. Run the *upgrade controller* command to upgrade controllers.
3. Once the controller is online, upgrade the APs in batches. Before initiating upgrade, ensure all APs are rebooted so that the uptime is less than 5 hours.

NOTE:

Fortinet recommends that you upgrade the 8.3.3 32-bit controller before upgrading the access points due to the issue mentioned in this section.
If KRACK patch is installed on the 8.3.3 32-bit controller then this recommendation does not apply. The controller can be directly upgraded to 8.4.

Upgrading a N+1 Site

To upgrade a site running N+1, all controllers must be on the same FortiWLC-SD version and the backup controller must be in the same subnet as the primary controllers.

NOTE:

- 64-bit controllers running pre-8.3.3 FortiWLC (except version **7.0-12**) are **required** to upgrade to the 8.3.3 GA version and then to the current 8.4.0 version.
- When upgraded to 8.3.3 GA, the N+1 setup needs to be reconfigured to enable N+1, that is, the master controller should be deleted and then added to the slave controller.
  This reconfiguration is not required when upgrading from 8.3.3 GA to 8.4.0.
- This issue does not exist on controllers with manufacturing build as 8.3.3 GA.

You can choose any of the following options to upgrade:

- **Option 1** - Just like you would upgrade any controller, you can upgrade a N+1 controller.
  1. Upgrade master and then upgrade slave.
  2. After the upgrade, enable master on slave using the *nplus1 enable* command.

- **Option 2** - Upgrade slave and then upgrade master.
  After the upgrade, enable master service on slave using the *nplus1 enable* command.

- **Option 3** - If there are multiple master controllers
  1. Upgrade all master controllers followed by slave controllers. After the upgrade, enable all master controllers on slave controllers using the *nplus1 enable* command.
  2. To enable master controller on slave controller, use the *nplus1 enable* command.
  3. Connect to all controllers using SSH or a serial cable.
  4. Use the *show nplus1* command to verify if the slave and master controllers are in the cluster.

     The output should display the following information:

     ```
     Admin: Enable
     ```

```
Switch: Yes
Reason: -
SW Version: 8.3-1
```

5. If the configuration does not display the above settings, use the *nplus1 enable <master-controller-ip>* command to complete the configuration.
6. To add any missing master controller to the cluster, use the *nplus1 add master* command.

Restore Saved Configuration

After upgrading, restore the saved configuration.

1. Copy the backup configuration back to the controller:
   ```
   # copy ftp://<user>:<passswd>@<offbox-ip-address>/runningconfig.txt orig-config.txt
   ```
2. Copy the saved configuration file to the running configuration file:
   ```
   # copy orig-config.txt running-config
   ```
3. Save the running configuration to the start-up configuration:
   ```
   # copy running-config startup-config
   ```

Upgrading Virtual Controllers

Virtual Controllers can be upgraded the same way as the hardware controllers. See sections Upgrading via CLI, Upgrading via GUI, and Upgrading a N+1 Site.
Download the appropriate Virtual Controller image from Fortinet Customer Support website.
For more information on managing the virtual controllers, see the *Virtual Wireless Controller Deployment Guide*.

Upgrading the controller can be done in the following ways:

- Using the FTP, TFTP, SCP, and SFTP protocols.
- Navigate to **Maintenance < File Management** in the FortiWLC GUI to import the downloaded package.

The following are sample commands for upgrading the Virtual Controllers using any of these protocols.

- upgrade-image tftp://10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar both reboot
- upgrade-image sftp://build@10.xx.xxx.xxx:/home/forti-x.x-xGAbuild-88-FWC1KD-rpm.tar both reboot
- upgrade-image scp://build@10.xx.xxx.xxx:/home /forti-x.x-xGAbuild-88-FWC1KD-rpm.tar both reboot
- upgrade-image ftp://anonymous@10.xx.xx.xx:forti-x.x-xbuild-x-x86_64-rpm.tar both reboot

The **both** option upgrades the Fortinet binaries (rpm) as well as the Kernel (iso), the **apps** option upgrades only the Fortinet binaries (rpm).

After upgrade, the Virtual Controller should maintain the System-id of the system, unless there were some changes in the fields that are used to generate the system-id. See the to the Licensing section for detailed information.

The International Virtual Controller can be installed, configured, licensed and upgraded the same way.

Upgrade Advisories

The following are upgrade advisories to consider before you begin upgrading your network.

NOTE:

Fortinet recommends upgrading a batch of maximum 100 APs.

Upgrading Virtual Controllers

In the upgrade command, select the options **Apps** or **Both** based on these requirements:

- Apps: This option will only upgrade the Fortinet binaries (rpm).
- Both: This option will upgrade Fortinet binaries as well as kernel (iso).

Upgrading FAP-U422EV

If the controller is running on pre-8.4.0 version and FAP-U422EV is deployed, follow these points:

- Disable *auto-ap-upgrade*.
  OR
- It is advised not to plug in FAP-U422EV till the controller gets upgraded to 8.4.0.

Mesh Deployments

When attempting to upgrade a mesh deployment, you must start upgrading the mesh APs individually, starting with the outermost APs and working inwards towards the gateway APs before upgrading the controller.

Feature Groups in Mesh profile

If APs that are part of a mesh profile are to be added to feature group, all APs of that mesh profile should be added to the same feature group. The Override Group Settings option in the *Wireless Interface* section in the *Configuration > Wireless > Radio* page must be enabled on the gateway AP.

Voice Scale Recommendations

The following voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all APs or SSIDs operating in that channel enhances voice call service. To enable:

1. In the WebUI, go to **Configuration > Devices > System Settings > Scale Settings** tab.
2. Enter a channel number in the *Voice Scale Channel List* field and click **OK**.

NOTE:

Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and this result in a noticeable reduction of throughput in data traffic.

New Features

This section describes the new hardware/software features introduced in this release of FortiWLC.

Fortinet Universal Access Points

The new Fortinet Universal Access Points (FAP-Us) are dual radio, dual band 802.11ac access points. These access points are designed to provide superior experience in data, voice, and video applications in enterprise class deployments.

FAP-U221EV and FAP-U223EV

The FAPs support two 2x2 MIMO radios (band locked) with a single core and comply with the IEEE 802.3af and 802.3at PoE specifications. A maximum of 8 ESS profiles and 128 clients are supported.

FAP-U24JEV

The FAPs support two 1x1 MIMO radios (band locked) with a single core and comply with the IEEE 802.3af and 802.3at PoE specifications. A maximum of 8 ESS profiles and 128 clients are supported.
The FAP has one 2x2 radio which will be always configured as two 1x1 interfaces.

NOTE:

FAP-U221EV, FAP-U223EV, and **FAP-U24JEV** do not support the following features:

- MU-MIMO
- LACP
- Hotspot2.0 – *Not supported in version 8.4.0 only.*
- Enterprise Mesh – *Not supported on FAP-U24JEV only.*
- Application Visibility (DPI)

FAP-U422EV

The FAP is a Wave-2 access point and supports two 4x4 MIMO radios (band locked) with a dual core. This device complies with the 802.3at PoE specifications. A maximum of 16 ESS profiles are supported.
The FAP supports all FortiWLC functionalities same as the FAP-U42xEV.

For more information on the FAPs, see the corresponding *Quick Start Guides*.

Enhancements

These are the enhancements in this release of FortiWLC.

- FAP-U422EV and AP832 are Passpoint R2 certified.
- In FortiWLC 8.4.0, the DFS is enabled for FAP-U32xEV FCC & Japan, FAP-U22xEV CE & Japan and FAP-U24JEV CE.
- The Simple Service Discovery Protocol (SSDP) is supported for Chromecast discovery.
- DNS configuration option is supported for FortiGate discovery.

Additional Information

This section describes information related to the usage of FortiWLC.

- To reduce multicast/broadcast traffic, Fortinet recommends enabling IGMP snooping on the Controller.
- Chromecast cast option is visible on the Youtube application only when the publisher or subscriber is in the tunneled mode.
- The capture-packets command with -R filer captures all packets instead of filtered packets.
- FortiWLC 8.4.0 supports versions A1 and A2 of BLE chips whereas FortiWLC 8.3.3 supports only version A1 of BLE.

Clients and Encryption Keys

These are the maximum supported clients and encryption/decryption keys for FAP models.

FAP Models	Maximum supported clients/radios			Encryption/Decryption			
		Native Cell		VCell		Native Cell	
	VCell	ARRP (Off)	ARRP (On)	Hardware	Software	Hardware	Software
FAP-U42x EV	170	170	256	170	0	256	0
FAP-U32x EV	170	170	256	170	0	256	0
FAP-U22x EV	128	128	128	64	64	64	64
FAP-U24J EV	128	128	128	64	64	64	64

VCell Roaming across Access Points

These are the supported VCell roaming details across APs.

Access Points	AP122	AP822	AP832	FAP-U22xEV	FAP-U32xEV	FAP-U42xEV	FAP-U24JEV
AP122	Supported	Supported	Supported with 2x2 MIMO mode	Supported with 2x2 MIMO mode	Supported with 2x2 MIMO mode	Supported with 2x2 MIMO mode	Supported with 1x1 mode
AP822	Supported	Supported	Supported with 2x2 MIMO mode	Supported	Supported with 2x2 MIMO mode	Supported with 2x2 MIMO mode	Supported with 1x1 mode
AP832	Supported with 2x2 MIMO mode	Supported with 2x2 MIMO mode	Supported	Supported with 2x2 MIMO mode	Supported	Supported with 3x3 MIMO mode	Supported with 1x1 mode
FAP-U22xEV	Supported with 2x2 MIMO mode	Supported	Supported with 2x2 MIMO mode	Supported	Not Supported	Not Supported	Supported with 1x1 mode
FAP-U32xEV	Supported with 2x2 MIMO mode	Supported with 2x2 MIMO mode	Supported	Not Supported	Supported	Supported with 3x3 MIMO mode	Not Supported
FAP-U42xEV	Supported with 2x2 MIMO mode	Supported with 2x2 MIMO mode	Supported with 3x3 MIMO mode	Not Supported	Supported with 3x3 MIMO mode	Supported	Not Supported
FAP-U24JEV	Supported with 1x1 MIMO mode	Supported with 1x1 MIMO mode	Supported with 1x1 MIMO mode	Supported with 1x1 MIMO mode	Not Supported	Not Supported	Supported

Fixed Issues

These are the fixed issues in this release of FortiWLC.

Bug ID	Description
453607	SNMP results were incomplete for neighboring APs count.
462374	In tunnel mode, STA did not communicate with the wired network after controller fail over.
464122	No framed IP attribute in the accounting start packet.
464687	wncagent spikes while running the event view, GUI and CLI failed to expose the event history.
470393	STA did not receive packets from the wired network after controller fail over.
473365	OAP433 crashes with kernel panic.
448391	The Search/Filter option not available for port profiles in the feature group configuration page of the FortiWLC GUI.
446850	The *conn ap* command co nnected to a different AP.
449185	AP CommNodeId duplicated in multiple APs.
452055	AP reboots with false *** FATAL ** Dead lock detected* error.
450379	Channel mismatch on some radios, with primary channel displayed as 44 and operating channel as 40.
457195	sys commands failed in the AP CLI.
455522	With Service Control enabled, the services crashed and restarted.
454144	Wncagent crashes after every one hour.
446296	AP sent Deauth to station by incorrect station type and unknown BSSID.
443669	An incorrect number of stations displayed in the pie charts on the system dashboard.
456464	Device connected but unable to pass traffic.
449409	Nplus1 was disabled when firmware was upgraded on FortiWLC-1000D,
452204	Random AP reboots with exception in APP visibility.
452650, 452649	FAP-U421EV did not auto-negotiate 1Gbps full duplex.
453317, 453316	Random AP832 crashes (NIP [c000d50c] e500_idle+0x90/0x94).
453511	Unable to configure DNS and domain name during the initial setup when the controller was on default setting.
457172	Controller based Captive Portal not working in the Bridged mode for AP822i.
457183	With IE9, incorrect page displayed for the Security Profiles Configuration.
460169	Channel mismatch on some radios, with primary channel displayed as 36 (Non- DFS channel) and operating channel as 100 (DFS Channel).
460587	Unable to edit ESS profiles from the web GUI.
461127	APs lost IP configuration after reboot and came up with default configuration.
446772	CP bypass page displayed even though the client is MAC authenticated and bypass enabled.
381008	Coordinator restarted due to memory issues
435490	All Chromecast devices did not show up in Youtube for casting.

423993	FAP-U421EV access points lost beacons in a virtual cell, causing clients to do assoc-2-assoc.
409488	Error in copying from backup configuration to running configuration.
422065	Controller not sending the RADIUS accounting packet.
462414	When the secondary DNS Server was configured, the secondary NetBIOS server gets the same IP address as the secondary DNS server.
448985	When controller fails over, OUI configuration of client_locater is not taken over to the new active controller.
449154	When the client_locator is enabled and the controller fails over, client_locator is disabled on the new active controller.
470643	Nplus1 configuration fails after firmware upgrade from 8.3 on FortiWLC-1000D.
470641	IP address on the slave controller is missing after firmware upgrade from 8.3 on FortiWLC-1000D.
466824	FAP-U321 upgrade fails.
469118	wncagent spikes observed.
470822	FAP-U421 reboots while unable to handle kernel null pointer - *LR is at wlc_scbfindband+0x5c/0x130 [wl].*
437223	The Console page in Chrome indicates that Adobe Flash is not installed even when it is installed in the Spectrum manager.
438782	Spectrum analysis: Overlay interference is misinterpreted as interference detected by the FAP.
436573	When upgrading from any prior release to 8.3.3, in N+1 configuration the passive slave controller Switch and Reason are No and No Config respectively. This issue occurs on 64-bit Controller models/instances.
470640	Radio Tx Freeze on FAP-U421EV & FAP-U423EV.
351641	[OAP-832] Frequent leaf node reboots with the LOST CONTACT with controller error.
475059	The controller IP address is set to 0.0.0.0 in the VPN administration page post upgrade to 8.4.0.
475307	[FAP-U42x] Radios' operating channel is different than the configured channel.
439721	High Latency and ping loss observed on clients configured in bridged mode with native and Static VLAN.

Known Issues

These are the known issues in this release of FortiWLC.

Bug ID	Description	Impact	Workaround
450682	Random FAP-U421EV crashes with kernel panic.	FAP reboots which impacts the client connectivity for the duration of AP boot up time.	
455780	In some MAC client devices authentication fails and the client is not able to connect. This is due to the delay in processing EAP-TLS messages.	This issue is specifically seen in MAC clients, due to the delay in EAP-TLS messages being processed by the AP, in some cases authentication fails because of which clients are not able to connect.	Set the authentication timeout to 3 seconds. For more information, contact the Customer Support.
461937	Sometimes, the FAP-U42x does not tag some packets on bridged data plane.	Data loss on wireless devices.	Connect the AP and run *sys perf off*.
463646	Sometimes in the FAP-U units, in high multicast/broadcast traffic, performance issues and high latency are observed in the bridged mode.	Latency in application usage for wireless clients.	Disable *Multicast-to-Unicast Conversion* option.
442046	[AP832] Sometimes, the APs do not respond to port 5000, client connectivity affected.	The AP reboots when this condition is encountered.	In 8.4.0, the AP auto reboots when this condition is encountered. For root cause fix, contact the Customer Support for installing the relevant patch.

474057	[Virtual FortiWLC] In case of a fresh FortiWLC installation, the gateway does not recognize the services in the FortiWLC GUI. In *Monitor > Service Control > Service Details*, the *Service* column is blank.	The Services pie chart in the Service Control Dashboard is not visible, unless the setup command is run or the controller is rebooted.	Run the *setup* command and reboot the controller.
474593	AP description with *sh* string gets lost post upgrade.	The AP description is set to default (AP ID).	Avoid using *sh* string in AP description.
453518	Difference in the AP signal strength on the 5Ghz band while operating in the normal mode and in the site survey mode (country code set to UK).	While doing site survey there will be a difference in signal strength if there is change in TX power other than values of 3 and 4.	Contact the Customer Support for installing the relevant patch.
466751	Sometimes, the APs reboot in a loop when trying to add new APs or doing a bulk reboot.	APs cannot discover the controller.	
462324	Sometimes, RADIUS requests are sent with the same port number for different IDs.	TLS errors for the clients see at RADIUS end. No impact on connectivity.	
463626	Round trip delays are observed randomly at wired side of AP822i after AP reboots.	Latency on wireless clients.	In 8.4.0, reboot the AP. For root cause fix, contact the Customer Support for installing the relevant patch.
456513	Sometimes, AP832 connected to Cisco WS-C2960X-48FPD-L comes up as 802.3af and not 802.3at with the BLE dongle.	BLE is disabled.	Contact the Customer Support for installing the relevant patch.

464308	APs Stuck in Disabled/Online state after reboot. This issue is observed under scale deployments, for example, rebooting 100+ APs at the same time.	Client connectivity affected till the AP reboots.	Reboot the AP.
464541	Wired Port profile in Mesh uplink port gets lost after upgrade to FortiWLC 8.4.0.	Wired clients cannot access the network.	Recreate the port interface for the AP.
475611	Multiple radio interfaces are created on the controller running FortiWLC 8.4.0.	False interface entries are created. Accessing the interface page from GUI is slow and interface related commands do not complete operation. In some cases, wncagent module might restart.	Contact the Customer Support.
476451	Sometimes in FAP-U22xEV and 24JEV, during high multicast traffic the APs reboot continuously with the *page allocation failure: low memory* error.	Client connectivity affected due to AP reboots.	Disable *Multicast-to-Unicast Conversion* option. Enable IGMP snooping on controller.

Known Issues in FAP-U422/FAP-U24J/FAP-U22xEV

Bug ID	Description	Impact	Workaround
451168	FAP-U24JEV/FAP-U22xEV- DTIM functionality is not working. PS-Poll based power-save clients fail to receive multicast traffic when the *Multicast-to-Unicast Conversion* option is disabled in the ESS profile.	Power-save clients fail to receive the multicast traffic sometimes and the battery life of wireless device is drained.	Enable the *Multicast-to-Unicast Conversion* option [Default setting].
453903	FAP-U24JEV – Client mitigation fails when the Rogue AP detection feature enabled.	Mitigation fails in cases of Rogue AP operating in foreign channel.	
474882	[FAP-U22x] Phy tx error with fatal error reinitializing and psm watchdog observed randomly on Radio 0/1 interface.	Data loss is observed when the error is reported till it recovers.	

Common Vulnerabilities and Exposures

This release of FortiWLC is no longer vulnerable to the following:

Bug ID	Vulnerability
450012	• CVE-2017-1000251 • CVE-2017-1000250
454662	• CVE-2017-13077 to CVE-2017-13082 • CVE-2017-13084 • CVE-2017-13086 to CVE-2017-13088
461748	CVE-2016-8491
443753	Broadcom ESDK vulnerability fix.

Visit *https://fortiguard.com/psirt* for more information.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service